Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Kyung H. Shin** **Group Art Unit 2143**	Facsimile No.: **703/872-9306**
From: Jennifer Pilcher Legal Assistant to Wayne Bailey	No. of Pages Including Cover Sheet: **26**

Message:

Enclosed herewith:

- Transmittal Document; and
- Appeal Brief.

Re: Application No. **09/692,348**
Attorney Docket No: **AUS9-2000-0631-US1**

Date: Tuesday, March 29, 2005

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Beukema et al.**

Serial No.: **09/692,348**

Filed: **October 19, 2000**

For: **Method and Apparatus for Reporting Unauthorized Attempts to Access Nodes in a Network Computing System**

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

§ Group Art Unit: **2143**
§
§ Examiner: **Shin, Kyung H.**
§
§ Attorney Docket No.: **AUS9-2000-0631-US1**
§

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on March 29, 2005.
By: Jennifer Pilcher
Jennifer Pilcher

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37).

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEY FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER

MAR 2 9 2005

Docket No. AUS9-2000-0631-US1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Beukema et al.**

Serial No. **09/692,348**

Filed: **October 19, 2000**

For: **Method and Apparatus for Reporting Unauthorized Attempts to Access Nodes in a Network Computing System**

§
§ Group Art Unit: **2143**
§
§ Examiner: **Shin, Kyung H.**
§
§
§
§

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on March 29, 2005.

By: Jennifer Pilcher
Jennifer Pilcher

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on January 31, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Businces Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-25

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-25
4. Claims allowed: None
5. Claims rejected: 1-25
6. Claims objected to: None

C. CLAIMS ON APPEAL

The claims on appeal are: 1-25

STATUS OF AMENDMENTS

No amendment after final was filed for this case.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

Claim 1 is directed to a method in a node for managing attempts to access such node. A packet is received from a source, where the packet includes a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node. A determination is made as to whether the packet is from a partition authorized to access the node by determining whether the partition key matches a second key for the node. If the first key does not match the second key, the packet is dropped without a response to the source. Information from the packet is stored, and sent to a selected recipient in response to a selected event. The above node access methodology is described in the Specification at page 23, line 1 – page 30, line 1 with reference to Figures 6-8 and with particular reference to Figure 8, elements 800-820.

Such multi-partitioning network advantageously provides an ability to segregate and selectively share devices, where some devices are private to a given node and others are shared between nodes (Specification page 23, lines 1-4). The claimed partition key advantageously provides an ability to determine which partitions can access a given node, as well as enable such segregation and selective sharing of devices in the multi-partitioning network.

B. CLAIM 10 - INDEPENDENT

Claim 10 is directed to a method in a node for reporting access violations. A packet is received from a source, where the packet includes authentication information that is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node. The received authentication information is verified to determine if the packet is from a partition authorized to access the node. If the received authentication information is unverified, the packet is dropped without a response to the source. Information from the packet is stored, and sent to a selected recipient in response to a selected event.

The above access violation methodology is described in the Specification at page 23, line 1 – page 30, line 1 with reference to Figures 6-8 and with particular reference to Figure 8, elements 800-820.

C. CLAIM 12 - INDEPENDENT

Claim 12 is directed to a data processing system comprising a bus system, a channel adapter unit connected to a system area network fabric, a memory connected to the bus system, wherein the memory includes as set of instructions; and a processing unit connected to the bus system. The processing unit executes the set of instructions to (i) receive a packet from a source, where the packet includes a first key that is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node; (ii) determine whether the first key matches a second key for the node; (iii) drop the packet without a response to the source if the first key does not match the second key; (iv) store information from the packet; and (v) send the information to a selected recipient in response to a selected event.

The above node access methodology and data processing system is described in the Specification at page 10, lines 9 – 17 and page 23, line 1 – page 30, line 1 with reference to Figures 1 and 6-8 and with particular reference to Figure 1, elements 102, 118, 120, 126, 128, 130, 132 and 134 and Figure 8, elements 800-820.

D. CLAIM 13 - INDEPENDENT

Claim 13 is directed to a node comprising a receiving means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for receiving a packet from a source, where the packet includes a first key that is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node. The node also comprises a determining means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node, a dropping means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for

dropping the packet without a response to the source if the first key does not match the second key, a storing means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for storing information from the packet; and a sending means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for sending the information to a selected recipient in response to a selected event.

The above node is described in the Specification at page 8, lines 1-11, page 26, lines 7-10 and page 23, line 1 – page 30, line 1 with reference to Figures 1 and 6-8 and with particular reference to Figure 1, elements 102 – 124, 158-166 and 172 and Figure 8, elements 800-820.

E. CLAIM 22 - INDEPENDENT

Claim 22 is directed to a node comprising a receiving means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for receiving a packet from a source, where the packet includes authentication information that is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node. The node also comprises a verifying means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for verifying the received authentication information to determine if the packet is from a partition authorized to access the node, a dropping means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for dropping the packet without a response to the source if the received authentication information is unverified, a storing means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for storing information from the packet, and a sending means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for sending the information to a selected recipient in response to a selected event.

The above node is described in the Specification at page 8, lines 1-11, page 26, lines 7-10 and page 23, line 1 – page 30, line 1 with reference to Figures 1 and 6-8 and with particular reference to Figure 1, elements 102 – 124, 158-166 and 172 and Figure 8, elements 800-820.

F. CLAIM 24 - INDEPENDENT

Claim 24 is directed to a computer program product in a computer readable medium for use in a node for managing attempts to access the node, the computer program product

comprising instructions for executing the steps recited in Claim 1. The explanation of the subject matter described with respect to Claim 1 above is hereby incorporated by reference.

G. CLAIM 25 - INDEPENDENT

Claim 25 is directed to a computer program product in a computer readable medium for use in a node for reporting access violations, the computer program product comprising instructions for executing the steps recited in Claim 10. The explanation of the subject matter described with respect to Claim 10 above is hereby incorporated by reference.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-4, 7-16 and 19-25)

Claims 1-4, 7-16 and 19-25 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Williams et al. (U.S. Patent No. 6,304,973) (hereinafter "Williams") in view of Frezza et al. (U.S. Patent No. 4,638,356) (hereinafter "Frezza") and further in view of MacKenzie et al. (U.S. Patent No. 6,363,495).

B. GROUND OF REJECTION 2 (Claims 5-6 and 17-18)

Claims 5-6 and 17-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Williams, in view of Frezza, further in view of MacKenzie as applied to claims 1 and 13 above, and further in view of Kekic et al. (U.S. Patent No. 6,664,978) (hereinafter "Kekic").

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-4, 7-16 and 19-25)

A.1. Claims 1-4, 8, 10-16 and 20, 22, 24 and 25

The cited MacKenzie reference (US Patent 6,363,495) has a filing date of January 19, 1999 and an issue date of March 26, 2002. The present application (Application 09/692,348) has a filing date of October 19, 2000. Thus, the cited McKenzie reference must be being used by the Examiner as a 35 USC 102(e)/103 reference. As the present application was filed after November 29, 1999, the provisions of 35 U.S.C. 103 (c), as amended by the American Inventors Protection Act of 1999 (enacted on November 29, 1999), apply. Appellants urge that the cited MacKenzie reference is disqualified as a valid reference, per the following:

> Application 09/692,348 and Patent 6,363,495 were, at the time the invention of Application 09/692,348 was made, owned by International Business Machines Corporation", and thus Patent 6,363,495 is disqualified as being a valid reference in a 35 USC 103 rejection, per 35 USC 103(c). See also MPEP 706.02(l)(1) and (l)(2).

Still further, Appellants urge error in the rejection of Claims 1, 10, 12, 13, 22, 24 and 25, as none of the valid references cited by the Examiner in rejecting such claims teach or suggest a multi-partitioned network, and receiving a packet that includes a partition key associated with a particular partition in the multi-partitioned network, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node (Claims 1, 12, 13, 24); or a multi-partitioned network, and receiving a packet that includes authentication information that is associated with a particular partition in the multi-partitioned network, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node (Claims 10, 22 and 25). Thus, a proper prima facie case of obviousness has not been established with respect to Claim 1[1], and the burden has not shifted to Appellants to

[1] To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or

rebut such improper obviousness assertion[2].

Still further, Appellants show that the cited Williams and Frezza references have been improperly combined using hindsight analysis. It is error to reconstruct the patentee's claimed invention from the prior art by using the patentee's claims as a "blueprint". When prior art references require selective combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight obtained from the invention itself. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 227 USPQ 543 (Fed. Cir. 1985). Because of the encryption technique described by Williams when exchanging messages between hosts, and the resulting requirement for encryption key exchange between the hosts *prior to* host message communication (Williams col. 20, lines 64-67; col. 21, lines 6-8), there would have been no motivation to also include a key as part of the message/packet, as transmitting a key along with the encrypted messages as taught by Williams would effectively defeat the entire purpose of Williams. Specifically, if a key was sent with the encrypted message, a network snooper (Williams Col. 7, lines 50-55) could capture the key/encrypted message and use such key to decrypt the accompanying message. Alternatively, if the key were not a key used as part of the encryption/decryption, there would be no reason to include such a key with the message as it would have no other purpose, and would degrade system performance by transmitting superfluous information. This establishes that there would have been no motivation to selectively combine the teachings of the cited references other than the motivation coming from the present patent application, which is improper hindsight analysis. *Interconnect Planning Corp. v. Feil, Id.*

A.2. Claims 7, 9, 19, 21 and 23

Appellants initially show error in the rejection of Claims 7, 9, 19, 21 and 23 for reasons

---

suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974). If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

[2] In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. Id.

given above with respect to Claims 1, 13 and 22, and show that (1) Application 09/692,348 and Patent 6,363,495 were, at the time the invention of Application 09/692,348 was made, owned by International Business Machines Corporation", and thus Patent 6,363,495 is disqualified as being a valid reference in a 35 USC 103 rejection, per 35 USC 103(c); (2) none of the valid references cited by the Examiner teach or suggest a multi-partitioned network, and receiving a packet that includes a partition key associated with a particular partition in the multi-partitioned network, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node (Claims 7, 9, 19, 21); or a multi-partitioned network, and receiving a packet that includes authentication information that is associated with a particular partition in the multi-partitioned network, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node (Claim 23); and (3) the cited Williams and Frezza references have been improperly combined using hindsight analysis.

Further with respect to Claim 7, such claim recites particular features of the multi-partitioned network, and in particular recites an ability to have devices being either private to a node or shared with one or more partitions. This claimed feature advantageously provides an ability to segregate and selectively share devices, where some devices are private to a given node and others are shared between nodes. In rejecting Claim 7, the Examiner states that this claimed feature is taught by Williams col. 27, lines 38-47. Appellants urge that this cited passage is merely standard 'boilerplate' that states that the Williams' invention is not limited to the specific examples disclosed therein. It does not describe any particular functionality with respect to a node, and in particular does not teach or otherwise suggest a node that comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network, as expressly recited in Claim 7. Therefore, a prima facie case of obviousness has not been established with respect to Claim 7, the burden has not shifted to Appellants to rebut such improper obviousness assertion, and Claim 7 is accordingly shown to have been erroneously rejected.

B. GROUND OF REJECTION 2 (Claims 5-6 and 17-18)

B.1. Claims 5-6 and 17-18

Appellants initially show error in the rejection of Claims 5-6 and 17-18 for reasons given above with respect to Claim 1, and show that (1) Application 09/692,348 and Patent 6,363,495 were, at the time the invention of Application 09/692,348 was made, owned by International Business Machines Corporation", and thus Patent 6,363,495 is disqualified as being a valid reference in a 35 USC 103 rejection, per 35 USC 103(c); (2) none of the valid references cited by the Examiner teach or suggest a multi-partitioned network, and receiving a packet that includes a partition key associated with a particular partition in the multi-partitioned network, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node; and (3) the cited Williams and Frezza references have been improperly combined using hindsight analysis.

Still further with respect to Claims 5-6 (and similarly for Claims 17 and 18), Appellants show error in such claim rejection as none of the valid references cited by the Examiner in rejecting such claims teach or suggest the claimed feature of "incrementing a counter source if the first key does not match the second key" (Claim 5) or "wherein the selected event occurs when the counter exceeds a threshold value" (Claim 6). In rejecting Claim 5, the Examiner cites Williams as teaching incrementing a source counter if the first key does not match the second key. Appellants initially show that since Williams does not teach any type of key matching, it therefore cannot teach incrementing a counter responsive to a key mismatch determination, as expressly recited in Claim 5. In addition, the passages cited by the Examiner in rejecting Claim 5 make no mention of any type of counter. Per Williams at Col. 18, lines 23-27, "security occurrences" are (1) displayed as real time alarms and (2) added to an audit log. Neither of these steps provides any sort of counting operation by a counter. As to Claim 6, the Examiner cites the same Williams passage used in rejecting Claim 5. As this passage does not teach any type of counter or counting, it similarly follows that there is no threshold value that when the counter exceeds such threshold value, the selected event occurs. Thus, Claims 5 and 6 (and similarly for Claims 17 and 18) are further shown to have been erroneously rejected as there are further missing claimed elements not taught or suggested by the cited references.

Appellants further show that Claims 5 and 6 (and similarly for Claims 17 and 18) do not stand or fall together for reasons given above regarding the occurrence of the selected event.

C. CONCLUSION

Appellants have thus shown substantial error in the final rejection of Claims 1- 25, and respectfully request that the Board reverse the rejection of such claims.

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method in a node for managing attempts to access the node, the method comprising:

receiving a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node;

determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node;

dropping the packet without a response to the source if the first key does not match the second key;

storing information from the packet; and

sending the information to a selected recipient in response to a selected event.

2. The method of claim 1, wherein the selected event is a request from the recipient for the information.

3. The method of claim 1, wherein the selected event is an occurrence of a trap.

4. The method of claim 1, wherein the selected event is a periodic event.

5. The method of claim 1 further comprising:

incrementing a counter source if the first key does not match the second key.

6. The method of claim 5, wherein the selected event occurs when the counter exceeds a threshold value.

7. The method of claim 1, wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network.

8. The method of claim 1, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address.

9. The method of claim 7, wherein the selected recipient is a subnet manager attached to a subnet that is responsible for configuring and managing switches, routers and channel adapters of the subnet.

10. A method in a node for reporting access violations, the method comprising:

receiving a packet from a source, wherein the packet includes authentication information, wherein the authentication information is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node;

verifying the received authentication information to determine if the packet is from a partition authorized to access the node;

dropping the packet without a response to the source if the received authentication information is unverified;

storing information from the packet; and

sending the information to a selected recipient in response to a selected event.

11. The method of claim 10, wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network.

12. A data processing system comprising:

a bus system;

a channel adapter unit connected to a system area network fabric;

a memory connected to the bus system, wherein the memory includes as set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node; determine whether the first key matches a second key for the node; drop the packet without a response to the source

if the first key does not match the second key; store information from the packet; and send the information to a selected recipient in response to a selected event.

13. A node comprising:

receiving means for receiving a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node;

determining means for determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node;

dropping means for dropping the packet without a response to the source if the first key does not match the second key;

storing means for storing information from the packet; and

sending means for sending the information to a selected recipient in response to a selected event.

14. The node of claim 13, wherein the selected event is a request from the recipient for the information.

15. The node of claim 13, wherein the selected event is an occurrence of a trap.

16. The node of claim 13, wherein the selected event is a periodic event.

17. The node of claim 13 further comprising:

incrementing means for incrementing a counter source if the first key does not match the second key.

18. The node of claim 17, wherein the selected event occurs when the counter source exceeds a threshold value.

19. The node of claim 13, wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network.

20. The node of claim 13, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address.

21. The node of claim 19, wherein the selected recipient is a subnet manager attached to a subnet that is responsible for configuring and managing switches, routers and channel adapters of the subnet.

22. A node comprising:

receiving means for receiving a packet from a source, wherein the packet includes authentication information, wherein the authentication information is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node;

verifying means for verifying the received authentication information to determine if the packet is from a partition authorized to access the node;

dropping means for dropping the packet without a response to the source if the received authentication information is unverified;

storing means for storing information from the packet; and

sending means for sending the information to a selected recipient in response to a selected event.

23. The node of claim 22, wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network.

24. A computer program product in a computer readable medium for use in a node for managing attempts to access the node, the computer program product comprising:

first instructions for receiving a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node;

second instructions for determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node;

third instructions for dropping the packet without a response to the source if the first key does not match the second key;

fourth instructions for storing information from the packet; and

fifth instructions for sending the information to a selected recipient in response to a selected event.

25. A computer program product in a computer readable medium for use in a node for reporting access violations, the computer program product comprising:

first instructions for receiving a packet from a source, wherein the packet includes authentication information, wherein the authentication information is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node;

second instructions for verifying the received authentication information to determine if the packet is from a partition authorized to access the node;

third instructions for dropping the packet without a response to the source if the received authentication information is unverified;

fourth instructions for storing information from the packet; and

fifth instructions for sending the information to a selected recipient in response to a selected event.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.